A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve personal health information (PHI), personally identifiable information (PII)

Common concept of a data breach

Data breaches may involve financial information such as credit card or bank details.

An attacker hacking into a corporate network to steal sensitive data.

EXAMPLES OF SECURITY BREACHES AND CORRESPONDING RECOMMENDED PRACTICES

Data Breach	Recommended Practice
Theft or loss: Computers and laptops, portable electronic devices, electronic media, paper files.	**Ensure proper physical security of electronic and physical restricted data wherever it lives.** Lock down workstations and laptops as a deterrent. Secure your area, files and portable equipment before leaving them unattended. Shred sensitive paper records before disposing of them. **Laptops should be secured at all times.** Keep it with you or lock it up securely before you step away -- and make sure it is locked to or in something permanent. **Use extra security measures for portable devices** (including laptop computers) and portable electronic media containing sensitive or critical info: Encryption Even portable devices and media with encrypted PII **Securely delete personal identity information (PII) and other restricted data when it is no longer needed for business purposes.**
Insecure storage or transmission of PII and other sensitive information: **Examples** PII, protected student records, or financial data being emailed in plain text, or sent in unprotected attachments. This puts data at risk should it be intercepted while in transit. Saving files containing PII or protected student data in a web folder that is publicly accessible online.	Be sure you know who has access to folders **before** you put restricted data there! Be certain you don't put sensitive information in locations that are publicly accessible from the Internet. Double check. If you can access it online without a password, so can others. Always transmit restricted data securely. This includes remote access and client/server transmissions. Don't email or IM (instant message) unencrypted restricted data. Don't forget about restricted data in attachments, screen shots, test data, etc. These need to be sent securely, as well.

Password hacked or revealed. This can lead to compromised data, compromised systems, and people using your accounts without your knowledge.	Use good, cryptic passwords that are difficult to guess, and keep them secure Never share or reveal your passwords, even to people or organizations you trust Use different passwords for accounts that provide access to restricted data than for your less-sensitive accounts. Use different passwords for work and non-work accounts. Change initial and temporary passwords, and password resets, as soon as possible whenever possible. These tend to be less secure.
Missing "patches" and updates: Hackers can take advantage of vulnerabilities in operating systems (OS) and applications if they are not properly patched or updated. This puts all of the data on those system and other connected systems at risk.	Make sure all systems connected to the network/Internet have all necessary **operating system (OS)** and **application** security “patches” and updates.
Computer infected with a virus or other malware: Computers that are not protected with anti-malware software are vulnerable. Out-of-date anti-malware may not detect known malware, leaving your computer vulnerable to infection.	Install anti-malware software and make sure it is always up-to-date. Don't click on unknown or unexpected links or attachments. These can infect your computer. Don’t open files sent via chat/IM or P2P software on a machine that contains restricted data – these files can bypass anti-virus screening.
Improperly configured or risky software: This can open your computer up to attackers.	Don't install unknown or suspicious programs on your computer. These can harbor behind-the-scenes computer viruses or open a “back door” giving others access to your computer without your knowledge. Don’t put sensitive information in places where access permissions are too broad.
Development server compromised: People sometimes think that "test" and "development" systems don't need to be as secure as "live" or "production" systems. This is a myth. If real data is used, it needs to be protected based on its level of sensitivity, regardless of what kind of system it is in. Otherwise it's an easy navigation for hackers.	Don’t use actual sensitive data in test or development systems, or for training purposes. If actual data is used, security for the system, test results (including screenshots), log files containing personal data, etc., must be equal to a comparable production system or data, including access controls. Truncate, de-identify or mask restricted data in these systems whenever possible.